Higher Ed Student Privacy Working Group Meeting Notes

Friday, September 29, 2017
11:30am-12:30pm
Topic: Gramm-Leach-Bliley Act (GLBA) Safeguards and Upcoming Higher Ed Audits

Dean Forbes (Sidley) on GLBA Safeguards

Department of Education Publications on Protecting Student Information

The DOE has issued a couple of publication on protecting student information. The publications serve as reminders to institutions of higher education and their 3rd party service providers of continuing obligations to protect data used in administering Title IV of the Federal student financial aid programs.

- DCL ID: GEN-15-18 (July 29, 2015)
- DCL ID: GEN-16-12 (July 1, 2016)

Those publication indicated that in order to support the Student Aid Internet Gateway (SAIG) enrollment agreement, that each institution agreed to. They had to put into place certain standards and best practices for managing personal information and information systems,and securing that information within those systems.

In particular, the Federal Student Aid (FSA), required the institutions to comply with the GBLA.

- Under Title V, financial services organizations, including institutions of higher education, are required to ensure that security and confidentiality of customer records and information.
- The requirement was recently added to the Program Participation Agreement (PPA), and it's reflected in the Federal Student Aid handbook.

The Department of Education plans to audit educational institutions for GLBA compliance, and the Department strongly encourages institutions to review and understand the standards defined in National Institute of Standards and Technology (NIST) SP 800-171.

Educational Institution Gramm-Leach-Bliley Act (GLBA) Safeguards Rule Compliance - Information Security Program

Each educational institution's PPA includes provisions requiring GLBA compliance.

Under the GLBA, financial services organizations, which include postsecondary educational institutions, are required to ensure the security and confidentiality of student financial aid records and information.

The GLBA also requires institutions to do the following:

- Develop, implement, and maintain a written information security program

- Designate the employee(s) responsible for coordinating the information security program; could be a Chief Information Security Officer, perhaps not with that title, but with that role
- Identify and assess risks to customer information
- Design and implement an information safeguards program
- Select appropriate service providers capable of maintaining appropriate safeguards, and
- Periodically evaluate and update their security program.

Educational Institution Presidents and CIOs should have, at a minimum:
- Evaluated and documented their their current security posture against GLBA's requirements
- Taken immediate action to remediate any identified deficiencies
- (Dean's comment): This demonstrates the role the Dept. of Education would like leadership to take within their own organization; showing initiative from the top down

The Department of Education has incorporated these GLBA security controls into Annual Audit Guide assess and confirm institutions' GLBA compliance, and they will require examination of evidence of GLBA compliance as part of institutions' annual student aid compliance audit.

GLBA Privacy and Safeguard Rules

The Gramm-Leach-Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999, requires financial institutions to:
- Explain their information-sharing practices to customers
- Limit sharing and disclosure of financial data with their parties
- Safeguard sensitive data

Gramm-Leach-Bliley Act:
- Requirement for initial and annual privacy notices
- Required options for information sharing
    - Some sharing does not require opt-out
        - "as permitted by law"
        - own advertising
        - joint marketing
    - Affiliate sharing (regulated by the FCRA)
        - sharing transaction & experience information
        - sharing creditworthiness information
        - sharing for affiliates' marking purposes
    - Sharing with non-affiliates
- New exception for annual notice requirement
    - applies only if the financial institution has a "no sharing" policy
    - applies only if the privacy policy has not changed from the prior communication

Safeguards

Title V of the GLBA sets out a number of mechanisms to protect the privacy and security of non-public personal information collected by financial institutions in connection with the provision of a financial product or service. REquires financial institutes to:

- provide notices of policies and practices regarding disclosure of personal information
- prohibit the disclosure of such data to unaffiliated third parties unless consumers are provided the right to "opt out" of such disclosure or unless other exceptions apply, and
- establish safeguards to protect the security of personal information

To Whom does the safeguards rule apply?

- the rule applies to "financial institutions" (see section 313.3(k) on applicability)
- all businesses, regardless of size, that are "significantly engaged" in providing financial products or services

What steps should your organization take to comply?

- The Safeguard Rules requires companies to:
    - assess and address risks to customer information
        - in all areas of their operations, including 3 areas important to information security:
            - employee management and training,
            - information systems, and
            - detecting and managing system failures.
    - determine what information they are collecting and storing, and whether they have a business need to do so
    - develop written information security plan:
        - which describes the program to protect customer information
        - is appropriate to company's size and complexity
        - outlines the nature and scope of its activities
        - is sensitive to the customer information it handles
        - designates one or more employees to coordinate its information security program
        - identifies and assesses the risks to customer information in each relevant area of the company's operation, and evaluates the effectiveness of the current safeguards for controlling these risks
        - designs and implements a safeguards program, and regularly monitors and tests it
        - selects service providers that can maintain appropriate safeguards, make sure your contract requires them to maintain safeguards, and oversees their handling of customer information, and
        - evaluates and adjusts the program in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.

Securing Personal Information

- Reasonable and appropriate security measures

Examples of Reasonable Security Measures:

- Checking references and background checks of employees with access to customer PII
- New hires agree to follow security measures
- Limit access based on role
- Access controls, including strong passwords
- Password activated screensavers
- Policies and procedures, including for mobile devices
- Training
- Remind employees of obligations
- Policy for telecommuters
- Imposing disciplinary measures
- No access for terminated employees
- Data asset inventory/data element inventory
- Secure data storage, transmission, and destruction
- Keep security controls up to date

FTC Orders and NIST

FTC orders regarding information security programs for two important reasons:

- Since 2002, the FTC has required several companies to put in place a comprehensive information security program that's based on the requirements of the GLBA safeguards rule
- The alignment with respect to NIST

FTC security cases typically require respondents to establish and maintain a comprehensive information security program that is reasonable designed to protect the security, confidentiality, and integrity of personal information accessible to end use.

The security program must contain administrative, technical, and physical safeguards appropriate to each respondent's size and complexity, the nature and scope of its activities, and the sensitivity of the personal information collected from or about consumers. Specifically, the orders require respondents to:

- Designate an employee or employees to coordinate and be accountable for the information security program
- Identify material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks
- Design and implement reasonable safeguards to control the risks identified through risk assessment, and regularly test or monitor the effectiveness of the safeguards' key controls, systems, and procedures
- Develop and use reasonable steps to select and retain service providers capable of appropriately safeguarding personal information they receive from respondents, and require service providers by contract to implement and maintain appropriate safeguards
- Evaluate and adjust the information security program in light of the results of the testing and monitoring, any material changes to the company's operations or business

arrangements, or any other circumstances that they know or have reason to know may have a material impact on the effectiveness of their information security program

Executive Order 13636 / NIST Cybersecurity Framework

- Executive Order 13636 : Improving Critical Infrastructure Cybersecurity (2/12/13)
    - "It is the policy of the U.S. to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties."
- NIST directed to work with stakeholders to develop voluntary framework for reducing cyber risks to critical infrastructure
- The Framework's compilation of practices is referred to as the "Core," which comprises 5 concurrent and continuous functions for managing cybersecurity risk:
    - Identity
        - Certain FTC cases have alleged that certain companies had failed to take appropriate actions to assess security risks and develop plans to address them (i.e. take reasonable steps to identify vulnerabilities and threats to determine the risk to consumers' personal information)
    - Protect
        - Certain FTC cases have alleged company failures to develop and implement reasonable information security safeguards and practices.
    - Detect
        - Certain FTC cases have alleged that companies have not had appropriate processes in place to monitor activity on their networks and detect intrusions - to reduce the risk of a data compromise or the breadth of compromise.
    - Respond
        - Certain FTC cases have challenged certain companies' failures to execute and maintain reasonable response processes and procedures, including breach detection and also taking appropriate steps when a breach occurs (i.e. contain events and communicate their occurrence with the appropriate parties)
    - Recover
        - The recover function supports a return to normal operations after a cybersecurity event. Certain FTC orders demonstrate the importance of this function, emphasizing how consumer interests should factor into a company's recovery plan.

Tiina Rodrigue (Dept. of Educaction) on Post-Secondary Institution Data-Security Overview and Requirements

Who needs to worry about data security?

- DOE usually reach out first to the President and Board of Directors/Regents because they are concerned with their data and everyone around them including the CIO, CISO, Staff, Faculty, students, and applications.

- Usually information security is adhoc at best and there is very little executive awareness.
- help schools to reduce their risks so that it's a more manageable level, and they realize that it may take schools years to do this
- schools are generally ignorant and don't know how to take steps to address this
- Educational institutions are specially being targeted because of the current state of ad-hoc security coupled with the educational environment being a rich trove of emails, information, and research.
- They will begin audition for GLB auditing, and they plan to start in FY 2018.
- so make sure that you have a security document and that you've annotated the person who is in control, and that you have safeguards and controls in place to manage those risks
- they will not be auditing some third party things

Why do I need to worry about data security?

Starting in FY18, GLBA information security safeguards will be audited to ensure administrative capability. Draft audit language:

- Audit Objectives- determine whether the IHE designated an individual to coordinate the information security program; performed a risk assessment that addresses the three areas noted in 16 CFR 314.4 (b) and documented safeguards for identified risks.
- Suggested Audit Procedure-
    - verify that the IHE has designated an individual to coordinate information security program
    - obtain the IHE risk assessment and verify that it addressed required areas noted in 16 CFR 314.4 (b).
    - Obtain the documentation created by the IHE

What are the data security requirements?

- Title IV schools are financial institutions per GLBA, 2002
- Per FSA PPA & SAIG Agreements, these schools must have GLBA safeguards in place. Schools without GLBA safeguards may be found administratively incapable (unable to properly administer Title IV funds.)
- GLBA Safeguard are:
    - Develop, implement, & maintain documented data security (info-sec) program
    - Designate an employee(s) to coordinate the program
- Identify reasonable foreseeable internal and external risks to data security via formal, documented risk assessment of:
    - Employee training and management
    - Information systems, including network and software design, as well as information processing, storage, transmission, and disposal
    - Detecting, preventing, and responding to attacks, instructions, or other systems failures
- Control the risks identified, by designing and implementing information safeguards and regularly testing/monitoring effectiveness
- Oversee service providers, by:

    - Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the FSA, student, & school (customer) information at issue
    - Requiring your service providers by contract to implement and maintain such safeguards
- Evaluate & adjust school's info-sec program in light of:
    - the results of the required testing/monitoring
    - any material changes to your operations or business arrangements
    - any other circumstances that you know may have a material impact on your information security program
- Title IV schools are subject to the requirements of the FTC Identity Theft Red Flags Rule (72 Fed. REg. 63718) issued on November 9th, 2007
- The "Red Flags Rule" requires an institution to develop and implement a written Identity Theft Prevention PRogram to
    - Detect
    - Prevent
    - Respond to patterns, practices, or specific activities that may indicate identity theft

What is a breach?
Per GLBA, a breach is any unauthorized disclosure, misuse, alteration, destruction or other compromise of information. (Comment by Tiina: Even if one record is compromised; it constitutes a breach. It can be a digital or hard copy record that's compromised.)

Here are some administrative, technical, and physical safeguards you can implement:
1) Ensure the security and confidentiality of customer information
2) Protect against any anticipated threats or hazards to the security or integrity of such records
3) Protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer

When do I report a breach?
- The Student Aid Internet Gateway (SAIG) Agreement requires that as a condition of continued participation in the federal student aid programs Title IV schools report suspected/actual data breaches
- Title IV schools must report **on the day of detection** when a data breach is even suspected
- The Department has the authority to fine institutions that do not comply with the requirements to self-report data breaches; up to $54,789 per violation per 34 C.F.R. § 36.2.
- The Department has reminded all institutions of this requirement through Dear Collegue Letters (GEN 15-18, GEN 16-12), electronic announcements, and the annual FSA Handbook.

How do I report a data breach?
1) Email cpssaig@ed.gov & copy your data breach team, executives, per your policy

a) Data to include in the email is listed below:
    i) Date of breach (suspected or known)
    ii) Impact of breach (# of records, etc)
    iii) Method of breach (hack, accidental disclosure, etc)
    iv) Information Security Program Point of Contact
        (1) Email and phone details with be necessary
    v) Remediation Status (complete, in process - with detail)
    vi) Next steps (as needed)
2) Call Education Security Operations Center (ED SOC) at 202-245-6550 with above data. ED-SOC is a 24/7 operation.
3) Call or Email Tiina Rodrigue - tiina.rodrigue@ed.gov or 202-377-3887 - of both methods fail.

How can you help me with data security?

- Institutions of Higher Education (IHE) Compliance Framework
    - Public-Private Partnership to reduce the burden of compliance for security and privacy controls for Title IV schools
    - Register for a free account to access the optional tool & data
    - Driven by the regulation on a federal and state level
    - Includes the international regulations for foreign schools
    - Consolidates all relevant laws into one compliance framework
    - Prevents duplicate effort, saving the schools money and effort

NIST has provide non-FISMA guidelines (800-171) that are recommended by FSA & Education in GEN 16-12 which gives specific technical standards to prove GLBA compliance:

- Access Control
- Awareness and TRaining
- Audit and Accountability
- Configuration Management
- Identification Authentication
- Incident Response
- Maintenance
- Media Protection
- Personnel Security
- Physical Protection
- Risk Assessment Requirements
- Security Assessment Requirements
- System and Communications Protection
- System and Information Integrity

As an option, you can contact Senior Advisor - Cybersecurity to:

- Ask hypothetical questions - is this an area of concern?
- Ger consultative review - policy or process (it's free!)
- Use the tools or get additional information (also free)
- Collaborate on best practices or bring ideas forward
- Review new Cybersecurity Compliance page -- send input to Tiina Rodrigue

What are my next steps?

- Find your information security policy and program for your school - if you don't have one, develop one
- verify your school's information security policy a program has an individual with his/her contact information -- Make sure to keep that person up to date on the policies and actively managing the program
- Verify that your school hs information risk assessment/testing schedule in place -- if you don't have one, develop one
- Verify that your school has documented the tests and results based on that schedule-- if haven't tested, have team start to follow the schedule and document it
- Add your information security policy/program/schedule/contact information to your consumer information and compliance website so that you can easily find/maintain it
- Communicate to your entire executive team so that if a breach happens, everyone is repared to respond immediate & appropriately

Question & Answer

Question: **How are schools supposed to implement these security measures with limited resources (funding & staff)? Are the requirements any different for community colleges?**

Answer: Design the program relevant to the size and scope of your school. Essentially a program that is reasonable and appropriate for your particular circumstance. NIST applies regardless of the size of the school so even places with limited budget and resources can and are expected to put controls in place mitigate issues. Schools with limited resources have the same expectation of controlling the data as large schools. They aren't expecting every school to have a million dollar solution. Making sure that you're taking the right steps to assess your risks...Just leverage the tools that we offer for free. Training is available in the non-profit spaces. With careful deliberation, you can do it...be mindful. Schools are expected to be mindful. Data is people, and if you are not being careful with the data then you are not being careful with people.

Question: **What are the responsibilities of companies that have contracts with schools?**

Answer: We expect third party service providers to follow the same requirements that the schools have. In other words, even if you have outsourced something, it does not obviate the school's responsibility over the data. Some of the flaws I've seen is that the contract is written so that the third party provider has more time than what is legally permissible. There are not only obligations with the Department of Education but there are obligations with state and federal laws. Make sure that those contractors will inform you promptly about anything that's going on that way they allow the school to report the breach on time. Furthermore, make sure that you're constantly reviewing and updating your agreements with the third party service providers. Recognize your obligations under state law. Work closely with Tiina and others. Make sure that GLBA is the basis of your contract with third-party service providers.

Question: **Could you speak to whether these requirements are also relevant to state agencies that collect institutional data?**

Answer: There are already limits under FERPA and HEA about what types of data can be shared. You're not supposed to share PII with state agencies unless they are distributing aid or part of that process. If you need specific advice, I recommend that you reach out to DOE's privacy technical center. If you are already sharing data with state agencies, I recommend that you review the legal requirements as they are constantly changing.